Microsoft®

Windows 2000® Server

Server Operating System

Planning and Managing FSMO Roles

Abstract

If you are responsible for the operational health of an Active Directory deployment with more than one domain controller, this paper is for you.

Active Directory supports multi-master update. But certain types of changes, such as schema updates, are impractical to perform in multi-master fashion. So in some cases only one domain controller, the holder of the *schema master role* in the case of schema updates, accepts schema updates and replicates them to other domain controllers.

The schema master role is one example of a flexible single-master operation (FSMO) role. This paper explains Active Directory's other FSMO roles, how you decide which domain controllers should hold FSMO roles, and how you respond when one of these domain controllers fails.

Note: This paper describes features of Windows 2000 Server Beta 3 and is not approved for general distribution outside of Microsoft. It can be shared with Windows 2000 Rapid Deployment Program customers who are under Non-Disclosure Agreements (NDA).

Revised 10 November 1998

© 1998 Microsoft Corporation. All rights reserved.

The information contained in this document represents the current view of Microsoft Corporation on the issues discussed as of the date of publication. Because Microsoft must respond to changing market conditions, it should not be interpreted to be a commitment on the part of Microsoft, and Microsoft cannot guarantee the accuracy of any information presented after the date of publication.

This White Paper is for informational purposes only. MICROSOFT MAKES NO WARRANTIES, EXPRESS OR IMPLIED, IN THIS DOCUMENT.

The BackOffice logo, Microsoft, Windows, and Windows NT are registered trademarks of Microsoft Corporation.

Other product or company names mentioned herein may be the trademarks of their respective owners.

Microsoft Corporation • One Microsoft Way • Redmond, WA 98052-6399 • USA

0X97 Part no. 098-XXXXX

CONTENTS

INTRODUCTION.....1

THE ROLES.....3
Schema Master 4
Domain Naming Master 4
RID Master 5
PDC Emulator 6
Infrastructure Master 7

PLACING ROLES.....9
Planning 9
Performing Role Transfer 10

RESPONDING TO FAILURES.....12
PDC Emulator 12
Infrastructure Master 13
Other Roles 13

CONCLUSION.....15
For More Information 15

INTRODUCTION

Active Directory supports multi-master update. This means you can make an update at any domain controller (DC) you can reach, even if that DC is disconnected from the rest of the network. At about the same time, someone somewhere else in the network might make an update that conflicts with yours. When network connectivity is restored, both updates will replicate. In spite of the conflicting updates, all DCs will eventually converge to the same value. This convergence process is called *conflict resolution*.

However, in some cases it is better to *prevent* conflicts than to resolve them after the fact. For instance, suppose that different DCs have conflicting versions of the directory schema. It is true that the schema conflict could be resolved using the same rules that Active Directory uses to resolve normal conflicts (roughly, "last writer wins.") But the schema is updated infrequently, and the consistency of the schema is very important. For the schema, conflict prevention is better than conflict resolution.

Therefore Active Directory performs updates to schema objects in single-master fashion. When necessary, administrators can shift the role of the server acting as the single master from one DC to another. But, only one DC in the entire directory, the one holding the *schema master role*, can accept updates to schema objects at a time.

The schema master role is one example of a flexible single-master operation role -- *FSMO role* for short. In Windows 2000 Server there are five different FSMO roles: schema master and four others. The schema master role controls schema updates, and each of the remaining four roles controls another specific set of changes that administrators make to the directory. For each role, only the DC holding that role can make the directory changes associated with that role.

In a small Active Directory deployment with a single domain controller, FSMO roles are not a consideration. But if you are responsible for the operational health of an Active Directory deployment with more than one domain controller, you need to know:

- When a domain controller holding a FSMO role is unavailable, what loss of functionality will administrators notice?
- Which domain controller or domain controllers should hold FSMO roles?
- When a domain controller holding a FSMO role is unavailable for an extended period, how should you respond to restore service?

This paper answers all these questions.

Active Directory defines five FSMO roles: *schema master*, *domain naming master*, *RID master*, *PDC emulator*, and *infrastructure master*. The schema master and domain naming master are per-directory roles (a

directory is sometimes called a "forest".) The other three are per-domain roles. So a directory with a single domain has five roles but a directory with more than one domain has more than five roles.

For example, in a directory acme.com with three domains

acme.com
na.acme.com
eur.acme.com

the total number of FSMO roles is eleven:

Schema master - directory acme.com

Domain naming master - directory acme.com

RID master - domain acme.com
RID master - domain na.acme.com
RID master - domain eur.acme.com

PDC emulator - domain acme.com
PDC emulator - domain na.acme.com
PDC emulator - domain eur.acme.com

Infrastructure master - domain acme.com
Infrastructure master - domain na.acme.com
Infrastructure master - domain eur.acme.com

A DC for any domain within a directory can hold a per-directory role for that directory; only a DC for a specific domain can hold a per-domain role for that domain. So a single DC can hold up to five FSMO roles, one of each. In the example, the eleven roles might be held by as few as three DCs or as many as eleven.

When you create the first Windows 2000 DC of a directory the system assigns all five roles to it; when you create the first Windows 2000 DC of a new domain in an existing directory the system assigns all three domain roles to it.

In a mixed-mode domain (e.g. those containing Windows NT Server 4.0 machines) only a Windows 2000 DC can hold FSMO roles.

Schema Master

To update the schema of a directory you must connect to the DC holding the directory’s schema master role. If the schema master is unavailable, you can’t update the schema.

To see if Active Directory Schema Manager is connected to the schema master, right-click the snap-in (in MMC’s left pane) and select “Operations Master …”. If the Current Focus and the Current Operations Master are the same, you are connected to the schema master. You must

also check the box “The Schema may be modified on this server” in order to enable schema changes.

If you attempt to modify the schema using Active Directory Schema Manager while connected to a DC that is not schema master, you’ll see a generic “attempted schema modification failed” error message.

Domain Naming Master

To add a domain to the directory (or remove a domain from the directory) you must connect to the DC holding the directory’s domain naming master role. If the domain naming master is unavailable, you can’t add or remove domains.

There are two ways of adding a domain to the directory:

- Using dcpromo. While creating the first domain controller of the domain, dcpromo contacts the domain naming master in order to create the domain. This technique requires the person running dcpromo to have sufficient privileges to create the domain.

  You’ll know that the domain naming master is unavailable when dcpromo displays the message

  ```
  Active Directory Installation Failed
  The operation has failed because
  To perform the requested operation, the Directory Service needs
  to contact the Domain Naming Master (server server05.acme.com).
  The attempt to contact it failed.
  The error was: “The specified server cannot perform the requested
  operation.”
  ```

  In this example server05.acme.com is the domain naming master.
- Using ntdsutil[1], then dcpromo. An administrator with sufficient privileges to add a domain to the directory can connect ntdsutil to the domain naming master to create the object[2] that names the new domain. This technique allows a less privileged person to run dcpromo and allows dcpromo to function without connecting to the domain naming master.

  You’ll know that the domain naming master is unavailable when ntdsutil fails to connect to the domain naming master:

  ```
  C:\>ntdsutil
  ntdsutil: domain management
  domain management: connections
  ```

[1] The Precreate subcommand of ntdsutil’s Domain management command.
[2] The object is a Cross-Ref object in the Partitions container of the Configuration NC.

```
server connections: connect to server05.acme.com
binding to server05.acme.com …
DsBindW error 0x6ba(The RPC server is unavailable.)
server connections:
```

RID Master

You can create a new User (or Group, or Computer) object[3] in a domain at any DC for that domain. However, after creating 512 User objects a DC must communicate with the DC holding the domain's RID master role before creating the next User object; then it is good for 512 more. If the RID master is unavailable you can't create the new User[4].

Using Active Directory Manager to create a new User, you'll know that the RID master is unavailable when Active Directory Manager displays the message

```
Active Directory Service
The object John Smith could not be created.
The problem encountered was:
The directory service has exhausted the pool of relative identifiers.
```

To move an object from one domain (the source domain) to another (the destination domain) using the MoveTree utility you must connect to the DC holding the source domain's RID master role. If the RID master is unavailable, you can't move objects to other domains.

[**XXX** What's the user experience when MoveTree fails because the RID master is unavailable?]

PDC Emulator

In a Windows NT 3.51 or Windows NT 4.0 system each domain contains a primary domain controller (PDC.) The functions of the PDC include processing password changes from both users and computers, replicating updates to backup domain controllers (BDCs), and running the Domain Master Browser. Windows 2000 inter-operates with Windows NT 3.51 and 4.0 workstations, member servers, and domain controllers. Therefore one domain controller in a Windows 2000 system, the one holding the PDC emulator role, serves as PDC for compatibility with older systems.

Active Directory is multi-master for most directory updates, so

[3] User, Group, and Computer objects are all examples of *security principal* objects.

[4] When a DC creates a security principal object it attaches a unique Windows NT Security ID (SID) to the object. A SID consists of a domain SID that is the same for all SIDs created in a domain, and a relative ID (RID) that is different for each SID created in a domain. The RID master allocates sequences of RIDs for use by the various DCs in a domain.

unavailability of the PDC emulator does not have the same impact as unavailability of the PDC in Windows NT. If the PDC emulator is unavailable, you lose services mentioned above.

[**XXX** What's the user/admin experience when (a) password change fails, (b) BDC replication fails, and (c) there's no domain master browser because the PDC emulator has failed?]

As older systems are upgraded, they cease to rely on the PDC:

- Windows 2000 clients (workstations and member servers), and downlevel clients that have installed the Windows 2000 distributed services client package, do not perform directory writes (e.g. password changes) preferentially at the PDC emulator; they use any DC for the domain.
- When all Windows NT 3.51 and 4.0 BDCs in a domain have upgraded to Windows 2000, the PDC emulator receives no downlevel replication requests.
- Windows 2000 clients (workstations and member servers), and downlevel clients that have installed the distributed services client package, use Active Directory to locate network resources. They don't require the Windows NT Browser service.

The PDC emulator role holder retains some functions in fully upgraded Windows 2000 domains. Password changes performed by other DCs of the domain are replicated preferentially to the PDC emulator. When an authentication fails with bad password at the other DCs of the domain, they forward the authentication request to the PDC emulator before failing, in case the password was recently changed. As a result, you are likely to experience an increased level of "password doesn't work" helpdesk calls when the PDC emulator is unavailable.

Infrastructure Master

Suppose you add a user to a group in the same domain using Active Directory Manager. Then, still connected to the same DC, you can open up the group to examine its members and will see the user you just added. If you then, still connected to the same DC, first rename the user and then display the group membership, you see the user's new name.

When the user and group are in different domains the behavior after a rename is less consistent. If after adding the user to a group in another domain you rename the user, the group does not see the rename right away. (In Active Directory Manager, selecting the Members tab of the group's property page will show the user's old name in the Name column.) This time lag is inevitable in a distributed system where sites function independently.

The infrastructure master of the group's domain is responsible for fixing up the group-to-user reference to reflect the rename. The infrastructure master performs its fixups locally and relies upon replication to bring all other replicas of the domain up to date. If the infrastructure master is unavailable, these fixups are delayed.

Planning

As described above, Windows 2000 performs an initial placement of roles on DCs. This placement works well for a directory deployed on a few DCs in a single site. In a directory with more DCs or multiple sites you plan the placement of FSMO roles to match your replication and network topologies.

Perform your planning domain by domain. If a domain has only one domain controller, that DC holds all the per-domain roles. Otherwise choose two domain controllers that are direct replication partners and well-connected by the network:

- To find the direct replication partners of a DC, use the Active Directory Sites and Services Manager. Locate the DC by browsing to the Sites container, to the site containing the DC, to the Servers container, to the DC's Server object. Expand the Server object to see the NTDS Settings object beneath it, and click the NTDS Settings object. The right pane displays a list of Connection objects. The From-Server attribute of each Connection object is a direct replication partner of this DC.
- If the two direct replication partner DCs you choose are in the same site they are well-connected. If they are in different sites, it is best for their sites to be connected via a network that's always available for replication, not one that's available for replication only at certain times of the day.

Call one of the two DCs you've chosen the *FSMO DC* for the domain, and call the other the *standby FSMO DC* for the domain. (You'll be using the standby FSMO DC in case of certain failures of the FSMO DC.)

In typical domains place both the RID master and PDC emulator roles on the FSMO DC. In a very large domain you can reduce the peak load on the PDC emulator by placing the RID master and PDC emulator roles on separate DCs, both direct replication partners of the standby FSMO DC. Keep the two roles together unless the load on your FSMO DC justifies the extra management burden of separating the roles.

Place the infrastructure master role on some DC for the domain that is not a GC server and that has a good network connection to some GC server (from any domain) – ideally the infrastructure master should be

within the same site as some GC server. If the FSMO DC meets these requirements, use it unless the load on your FSMO DC justifies the extra management burden of separating the roles.

When you've planned all of the per-domain roles it is time to consider the per-directory roles. These two roles (schema master and domain naming master) should always be placed on the same DC. Place both roles on a DC that's close to the person or group responsible for schema updates and the creation of new domains. To simplify management you can place these roles on the FSMO DC of some domain.

In most cases your role placement plan will not require changes as your directory grows. Normally you just leave your role placements alone. But when you plan to decommission a DC, reduce the connectivity of your network, or change the GC server status of a DC, you need to review your plan and revise it as necessary.

Performing Role Transfer

To *transfer* a role is to move it with the cooperation of its current holder. Given a role placement plan you need to transfer each role from its default location to its planned location. Depending upon the role, you perform role transfer using one of three Active Directory MMC snap-ins:

- schema master: Active Directory Schema Manager
- domain naming master: Active Directory Tree Manager
- per-domain roles: Active Directory Manager

To transfer a role, first focus the snap-in on the domain controller that should receive the role. Then right-click the left-pane snap-in object and select "Operations Master ..." from the context menu. For per-domain roles you then select the tab corresponding to the specific role you want to transfer. The property page displays both the "Current Focus" (the DC that the snap-in is focused on), the "Current Operations Master" (the DC that's the current role holder) and the online/offline status of the current role holder. Click "Change..." and click "OK" on the confirm dialog.

If the current role holder is available the transfer will complete in a few seconds. See below for what to do if the current role holder is not available.

You'll notice the unavailability of a FSMO role holder by trying and failing to perform some role-controlled function. For instance, you try to modify the schema at the schema master, but can't connect. Or you try to transfer the infrastructure master role to a new DC (before making the current infrastructure master a GC server) but the transfer fails.

In either case your first step is to determine the cause and expected

length of the outage. Is the problem in the network, or is the DC down? Is it a hardware problem or a software problem?

If the cause is a networking problem, or a server that will restart soon, you simply wait for the role holder to become available again before performing your function.

To *seize* a role is to move it without the cooperation of its current holder. In general you try to avoid seizing roles, but sometimes seizing is the right thing to do. The decision depends upon the role and the expected length of the outage.

PDC Emulator

The PDC emulator role is unique because its loss can be visible to end-users, not just to administrators. Therefore when the PDC emulator is unavailable you may need to fix the problem more quickly than with other roles.

If the PDC emulator goes offline for a significant period, and the domain has downlevel workstations that have not installed the Windows 2000 distributed services client package or has downlevel DCs, seize the PDC emulator role to the standby FSMO DC you've planned.

The user interface for this seizure is just like that for a normal transfer, but requires an extra confirmation from you. You should say "OK" to the confirmation only in this specific situation where you know the current PDC emulator will be offline for a significant period. Later, when the original PDC emulator DC comes back online, transfer the role back.

Infrastructure Master

Temporary loss of a domain's infrastructure master is not visible to end-users, and won't even be visible to many administrators unless you've recently moved or renamed a lot of accounts. Therefore this often isn't a problem worth fixing.

If you anticipate a very long outage of a domain's infrastructure master and want to fix the problem, first select a DC that's not a global catalog and that has a good network connection to some GC server (from any domain) – ideally within the same site as a GC server. It is *not* important that the new infrastructure master be near the previous one. Then seize the infrastructure master role to the DC you've selected.

The user interface for this seizure is just like for a normal transfer, but requires an extra confirmation from you. You should say "OK" to the confirmation only in this specific situation where you know the current infrastructure master will be offline for a very long period. Later, when the original infrastructure master DC comes back online, transfer the role

back.

Other Roles

Temporary loss of schema master, domain naming master, or RID master is not visible to end-users, and won't be visible to most administrators. Therefore this usually isn't a problem worth fixing.

If you anticipate an extremely long outage of the DC holding one of these roles, you can seize that role to the standby FSMO DC you've planned. However seizing any of these roles is a drastic step that you'd normally take only when the outage is *permanent*, i.e. the DC has been physically destroyed and cannot be restored from backup media.

A DC whose schema master, domain naming master, or RID master role has been seized must never come back online. You should ensure that the outage of this DC will be permanent (e.g. by disconnecting the DC from the network) before proceeding with role seizure.

The DC that will seize the role must be fully up to date with respect to updates performed on the previous role holder. Use the repadmin tool (winnt\support\reskit\netmgmt\dstools\repadmin.exe) to check this condition. For instance, suppose that server05 is the RID master of domain acme.com, server10 is the standby FSMO DC, and server12 is the only other DC of domain acme.com. You'd issue the two commands

```
C:\>repadmin /showvector dc=acme,dc=com server10.acme.com
New York\server05       @ USN 0x26F4
San Francisco\server12  @ USN 0x27E6

C:\>repadmin /showvector dc=acme,dc=com server12.acme.com
New York\server05       @ USN 0x259F
Chicago\server10        @ USN 0x311D
```

Ignore all the output lines except those for server05. Since server10's up-to-dateness with respect to server05 (server05 USN `0x26F4`) is larger than server 12's up-to-dateness with respect to server05 (server05 USN `0x259F`), it is safe for server10 to seize the RID master role formerly held by server05. If server10 had been less up-to-date with respect to server05 than server12, you'd either wait for normal replication to update server10, or use repadmin /sync /force to make the replication happen immediately.

Once you are ready to seize the role, use ntdsutil as in the following example:

```
C:\>ntdsutil
ntdsutil: roles
fsmo maintenance: connections
```

CONCLUSION

```
server connections: connect to server10.acme.com
binding to server10.acme.com …
Connected to server10.acme.com
  using credentials of locally logged on user
server connections: quit
fsmo maintenance: seize RID master
Server "server10.acme.com" knows about 5 roles
Schema - CN=NTDS Settings,CN=server04,CN=Servers,
  CN=New York,CN=Sites,CN=Configuration,DC=acme,DC=com
Domain - CN=NTDS Settings,CN=server04,CN=Servers,
  CN=New York,CN=Sites,CN=Configuration,DC=acme,DC=com
PDC - CN=NTDS Settings,CN=server10,CN=Servers,
  CN=Chicago,CN=Sites,CN=Configuration,DC=acme,DC=com
RID - CN=NTDS Settings,CN=server10,CN=Servers,
  CN=Chicago,CN=Sites,CN=Configuration,DC=acme,DC=com
Infrastructure – CN=NTDS Settings,CN=server12,CN=Servers,
  CN=San Francisco,CN=Sites,CN=Configuration,DC=acme,DC=com
fsmo maintenance: quit
ntdsutil: quit
C:\>
```

As someone responsible for the operational health of an Active Directory deployment, you should build an understanding of FSMO roles into your plans and procedures. By doing so you'll reduce or eliminate potential problems.

For More Information

For the latest information on Windows NT Server, check out our World Wide Web site at http://www.microsoft.com/ntserver the Windows NT Server Forum on the Microsoft Network (GO WORD: MSNTS).